GSA

Customer - Industry Partner Meeting

June 12, 2002
Kansas City

Rich Wilhelm
Vice President

The view from 80,000 feet…

- **My background**
  - Former U.S. Intelligence Community Senior and White House Staff
  - Focus Watch & Warning; Crisis & War; Preparedness; Information/Infrastructure Protection
- **As former Executive Director, Intelligence Community**
  - I was able to gain unique perspectives
  - I have ‘guilty knowledge’…

    …an awareness of the art of the possible cyber attacks & terrorism
  - Five years in private sector to understand business side
- **My conclusions:**
  - **Security has become a key critical factor in business continuity & opportunity capture for future success**
  - **Broad corporate risk management response is most often is the key**

My Message

- The World Is More Complicated and So Therefore Is Risk Management

- We Often Look To Technology To Solve Our Most Pressing Security Problems, But It Is Most Often Leadership, Perspective , Management and Coordination Which Are Far More Important

- The Big Winners Will Be Firms and Agencies Which Take the Broadest View of Risk Management, Integrating Not Only Traditional Security Disciplines But Also Other Areas of Risk and Connecting Them To the Business and Its Mission

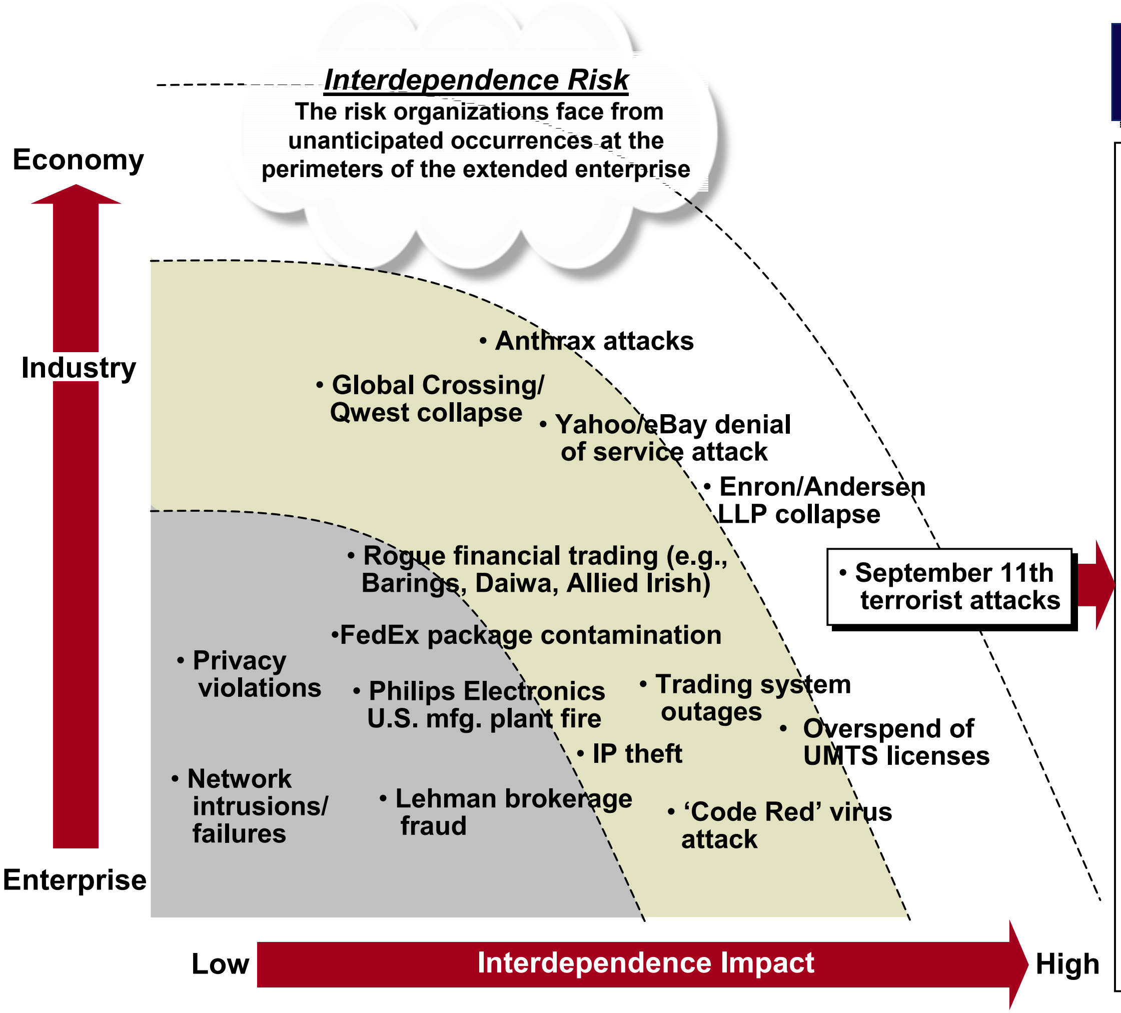
Risk Management:

It's a complicated world

***ONE EXAMPLE*:**

The Macro View

Recent history has proven that single events can have profound impacts and the cascading discontinuities result from unrecognized interdependencies



Interdependence Risk
The risk organizations face from unanticipated occurrences at the perimeters of the extended enterprise
Economy
Industry
Enterprise
• Anthrax attacks
• Global Crossing/ Qwest collapse
• Yahoo/eBay denial of service attack
• Enron/Andersen LLP collapse
• Rogue financial trading (e.g., Barings, Daiwa, Allied Irish)
•FedEx package contamination
• Privacy violations
• Philips Electronics U.S. mfg. plant fire
• Trading system outages
• Overspend of UMTS licenses
• IP theft
• Network intrusions/ failures
• Lehman brokerage fraud
• 'Code Red' virus attack
• September 11th terrorist attacks
Low
Interdependence Impact
High

Interdependence Risk Consequences of September 11th

- Deepening of US recession
- Decline in consumer confidence and buying
- US airline industry incurs multi-billion dollar losses
- Industry restructuring (e.g., accounting, airlines)
- Loss in confidence in security of public infrastructure
- National, state and local economies falter from tourism shutdown
- Decline in key services and customer traffic force businesses into bankruptcy
- Lost revenue, market share and market value
- Closed borders delay delivery schedules and increase distribution and inventory holding costs
- Production lines halted with grounding of air-freighted materials

Interdependence risk is highlighted by the roles that industries play in providing security and continuity to the economy ...

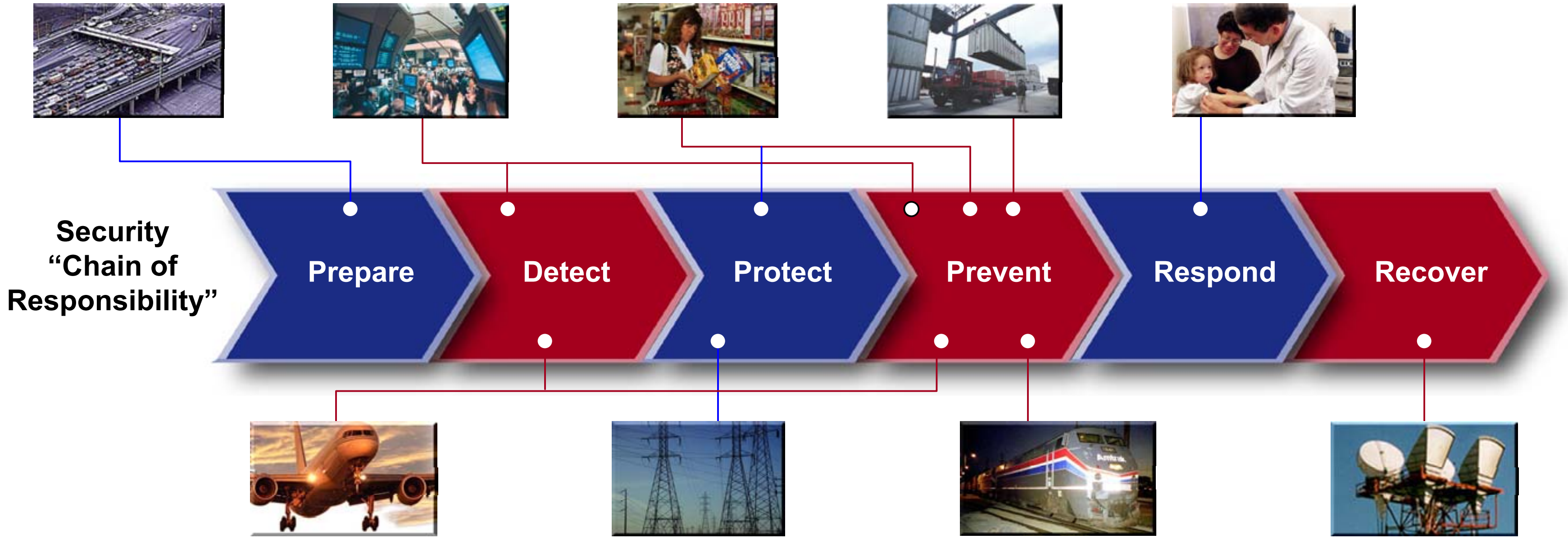
Public Infrastructure - Prepare contingency plans for disruption to traffic infrastructure

Financial Services - Detect illicit funds flows and prevent harm to capital markets

Consumer Products - Prevent systematic contamination of key consumer goods

Shipping - Prevent contaminated material from entering shipment flows

Health Care - Establish plans/ measures to respond to health-related attacks



Security "Chain of Responsibility"

Prepare

Detect

Protect

Prevent

Respond

Recover

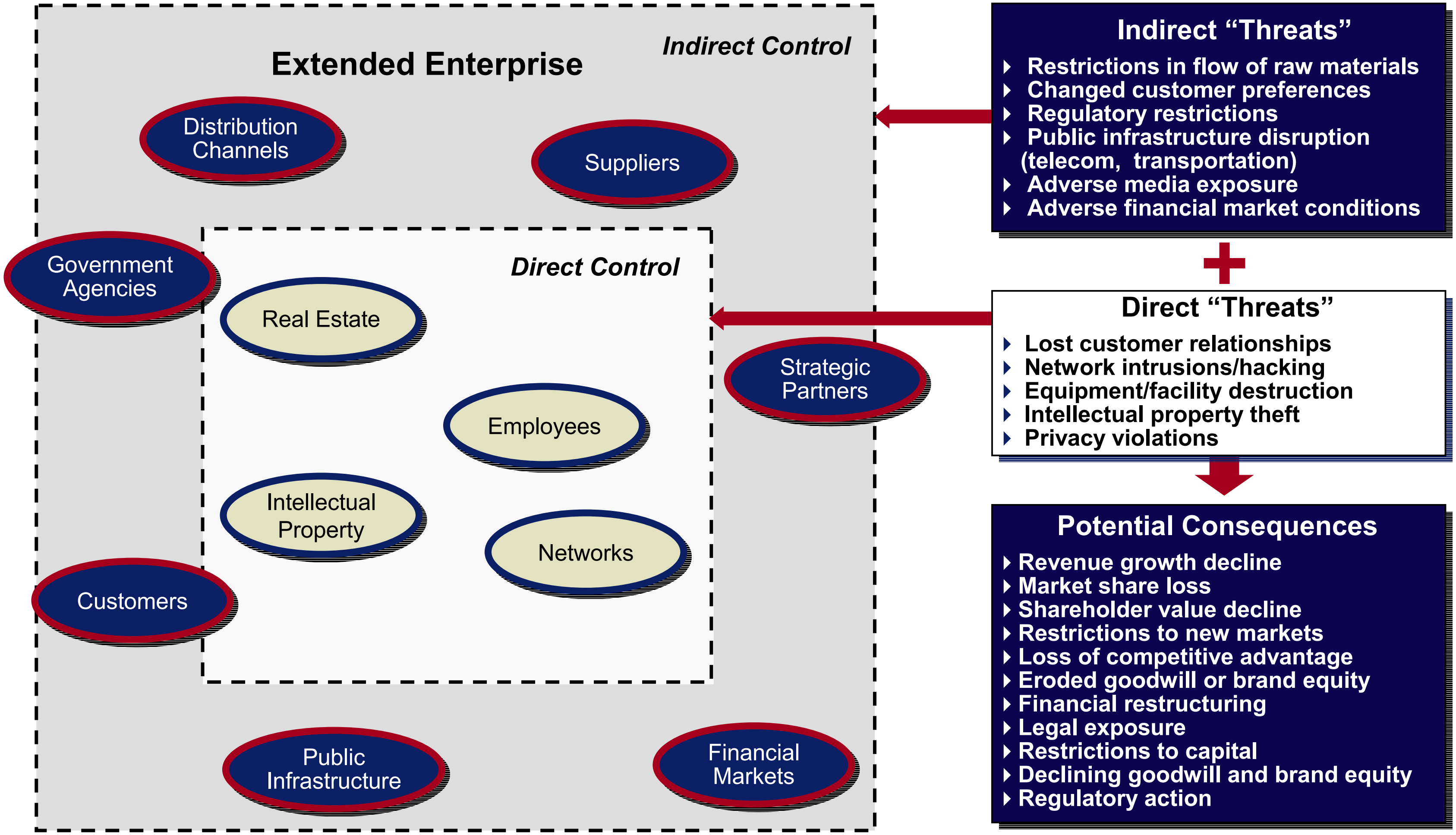
Airlines - Develop measures to detect and prevent security breaches

Energy - Protect against damage to critical infrastructure

Public Transportation - Prevent damage to public transportation facilities and passengers

Telecom - Provide the ability to recover/restore vital communications services

…which, while essential to growth and profitability, expose firms and agencies to risks they cannot control directly



Extended Enterprise

Indirect Control

Distribution Channels

Suppliers

Government Agencies

Direct Control

Real Estate

Employees

Intellectual Property

Networks

Strategic Partners

Customers

Public Infrastructure

Financial Markets

Indirect “Threats”

- Restrictions in flow of raw materials
- Changed customer preferences
- Regulatory restrictions
- Public infrastructure disruption (telecom, transportation)
- Adverse media exposure
- Adverse financial market conditions

+

Direct “Threats”

- Lost customer relationships
- Network intrusions/hacking
- Equipment/facility destruction
- Intellectual property theft
- Privacy violations

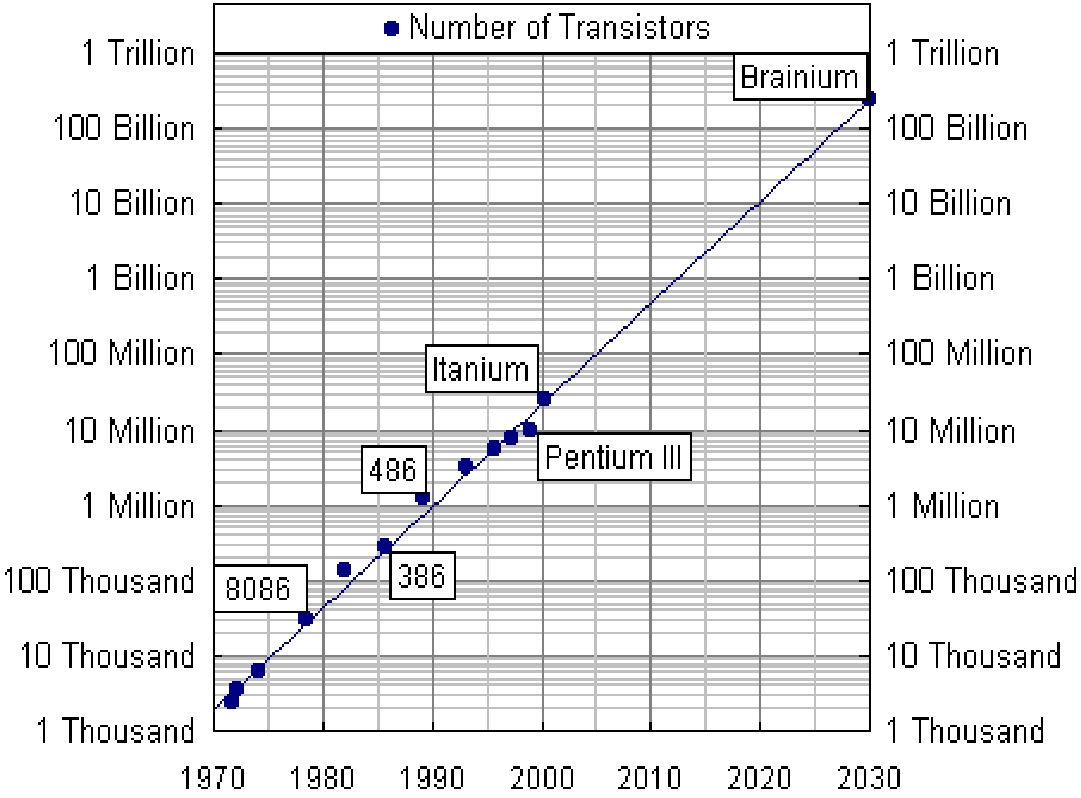
Potential Consequences

- Revenue growth decline
- Market share loss
- Shareholder value decline
- Restrictions to new markets
- Loss of competitive advantage
- Eroded goodwill or brand equity
- Financial restructuring
- Legal exposure
- Restrictions to capital
- Declining goodwill and brand equity
- Regulatory action

Another Example:

Technology and the Destructive Power of Terrorists

Hypothesis: The destructive power of the (cyber) terrorist doubles every 18 months (Giorgio's Corollary to Moore's Law)

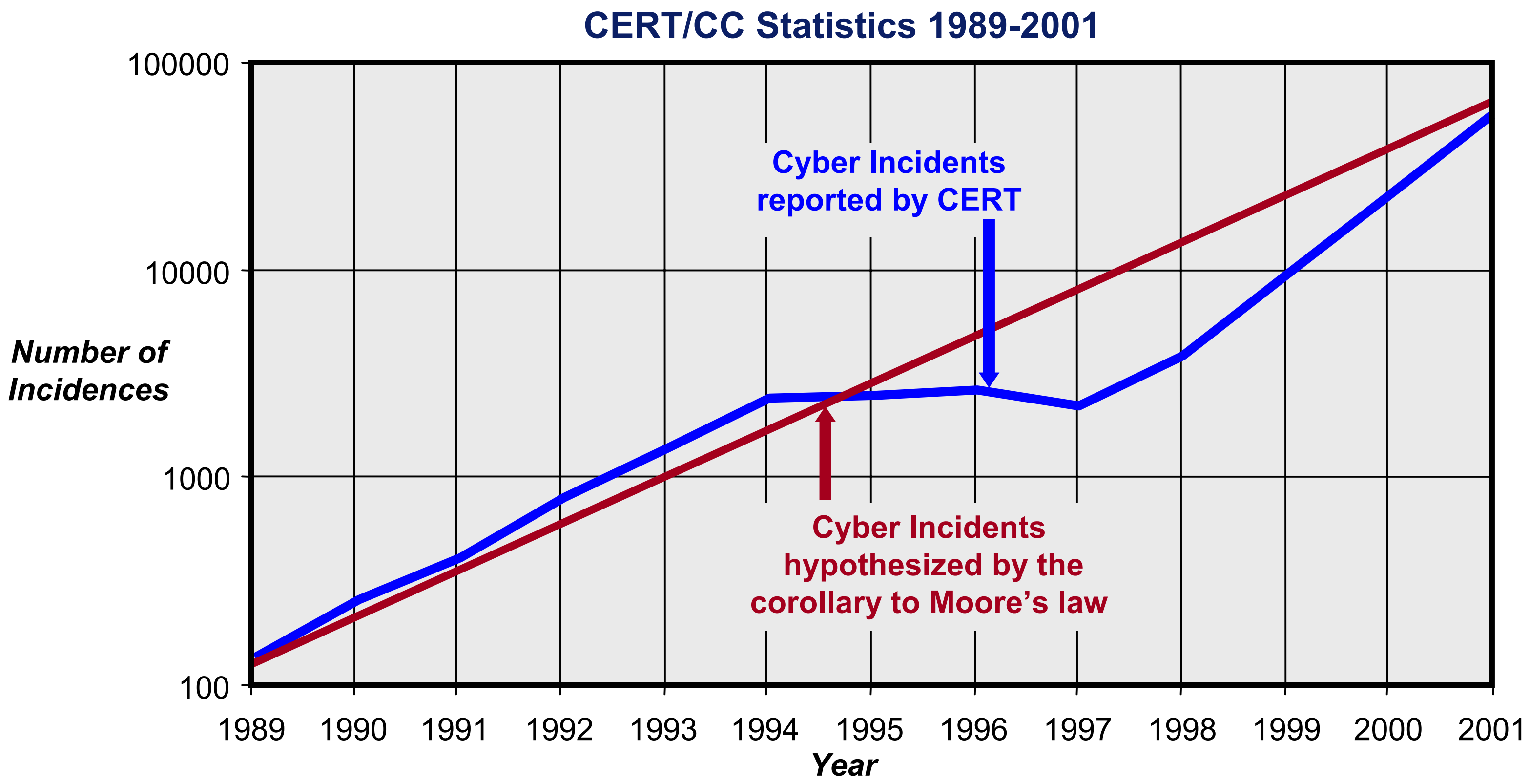


Implications

- Better collection on potential terrorist targets and better data mining capabilities
- Better planning tools
- Faster and more flexible communication capabilities
- Better, faster and more available encryption
- Access to multiple media coverage through internet streaming video

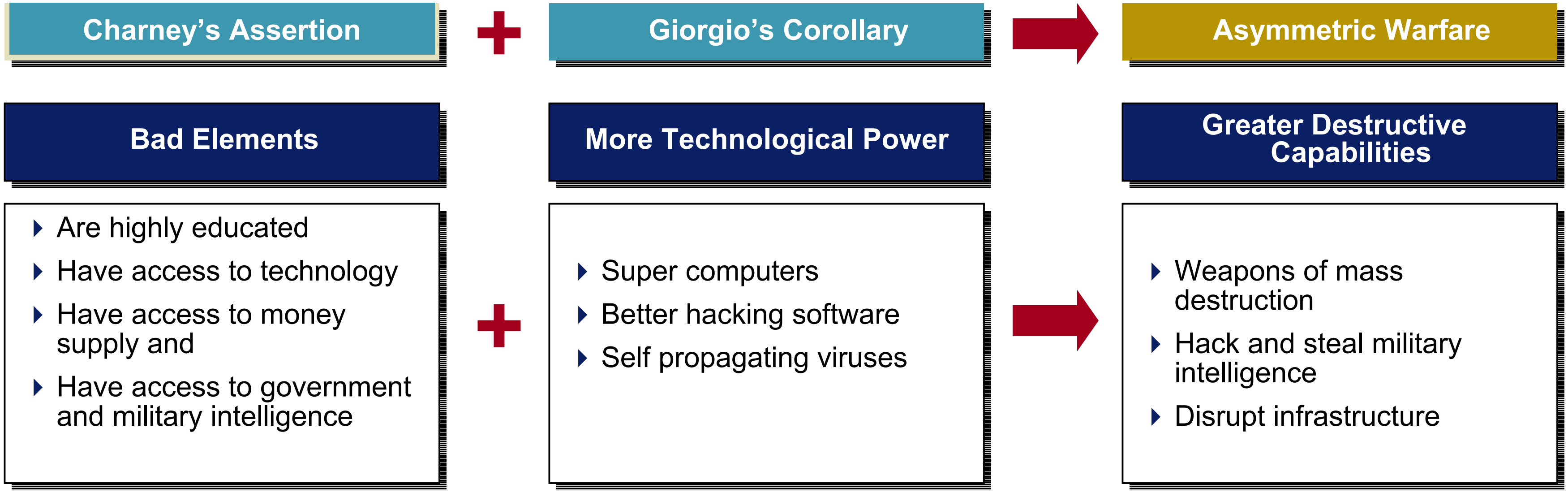
Decreasing Cost → **Increasing Dependency** → **Increasing Destructiveness**

Cyber attacks over the past few years prove that we have a problem…and they have followed a growth pattern remarkably similar to Moore’s law.



The Computer Emergency Response Team Coordination Center at Carnegie Mellon University tracks the number of reported hacking incidents.

Bad elements with more technological power implies potentially greater destructive capabilities



Charney's Assertion + **Giorgio's Corollary** → **Asymmetric Warfare**

Bad Elements + **More Technological Power** → **Greater Destructive Capabilities**

Bad Elements

- Are highly educated
- Have access to technology
- Have access to money supply and
- Have access to government and military intelligence

More Technological Power

- Super computers
- Better hacking software
- Self propagating viruses

Greater Destructive Capabilities

- Weapons of mass destruction
- Hack and steal military intelligence
- Disrupt infrastructure

> ***"There will always be some percentage of the population which is up to no good"***
>
> *Scott Charney (former Computer Crime and Intellectual Property Section (CCIPS) at DOJ)*

Technology was a major enabler in what could be perceived as a low tech terrorist attack

35 Year old (low) technology….

Enhanced by modern technology

- Better intelligence gathering
  - Computer in caves
  - Instant communications
- Better training and planning tools
  - Flight simulator
  - Flight schedules through Travelocity
- Ease of communication
- Better encryption
  - Hypothesized use of images to transmit hidden messages
- Higher media coverage
  - CNN coverage available worldwide through internet

Security:

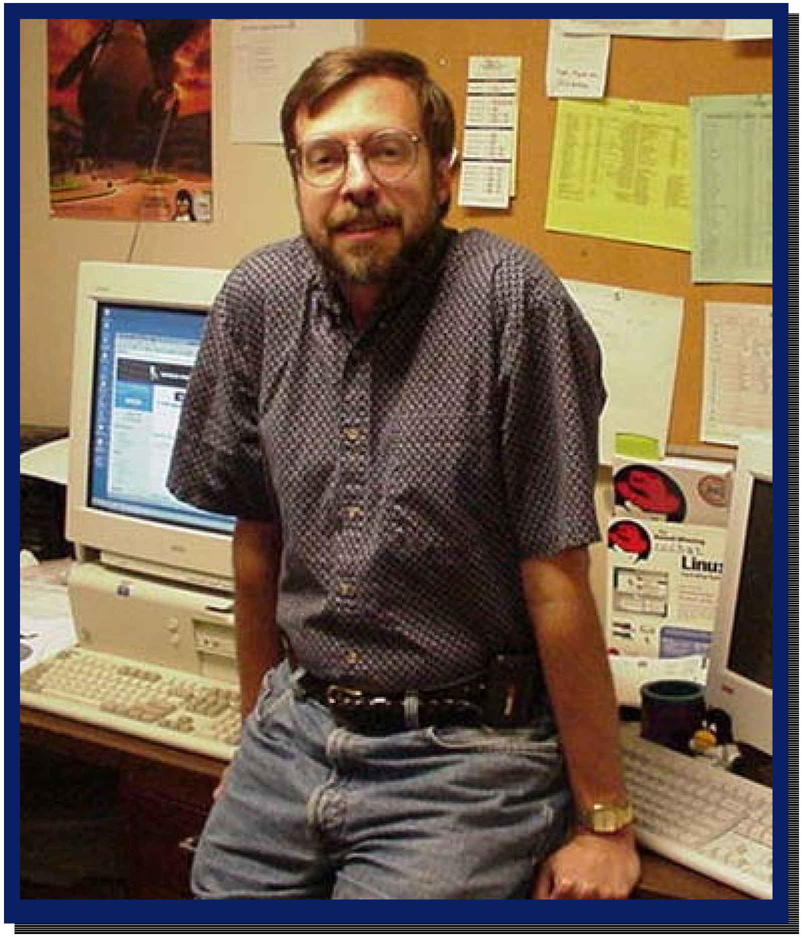
“The way we have traditionally been”

Let me introduce you to some of the traditional “players”

This is Joe. He does Physical Security.

- Retired policeman, maybe with some prior military experience
- Checks badges, knows alarms, guards the gates
- Knowledge of computer security limited to checking property passes when they leave the building
- Rules of engagement for use of weapon probably unclear
- Loyal, competent, but narrowly focused
- Likes formal rules, clear guidance

This is Bill. He does Information Security.



- He’s a geek, maybe even a little bit of a nerd.
- Has 13 computers in his basement at home, creates his own networks there and dares hackers to break into them.
- Works for the CIO who may not be very influential in the organization
- Speaks in a technical language which is often inaccessible to the common man
- Tends toward informality, and prefers technical solutions over management ones
- Kind of lives in his own world

This is Mary. She maintains your personnel and Personnel Security records.

- "Checks the blocks"
- Processes the paper, the supreme bureaucrat, nothing gets by her
- Has little understanding of the jobs requiring personnel reliability background checks that she performs
- In a particular sense, she is very unfamiliar with computer security
- But loyal and competent in the world she controls

This is Josephine. She is the Business Continuity person.

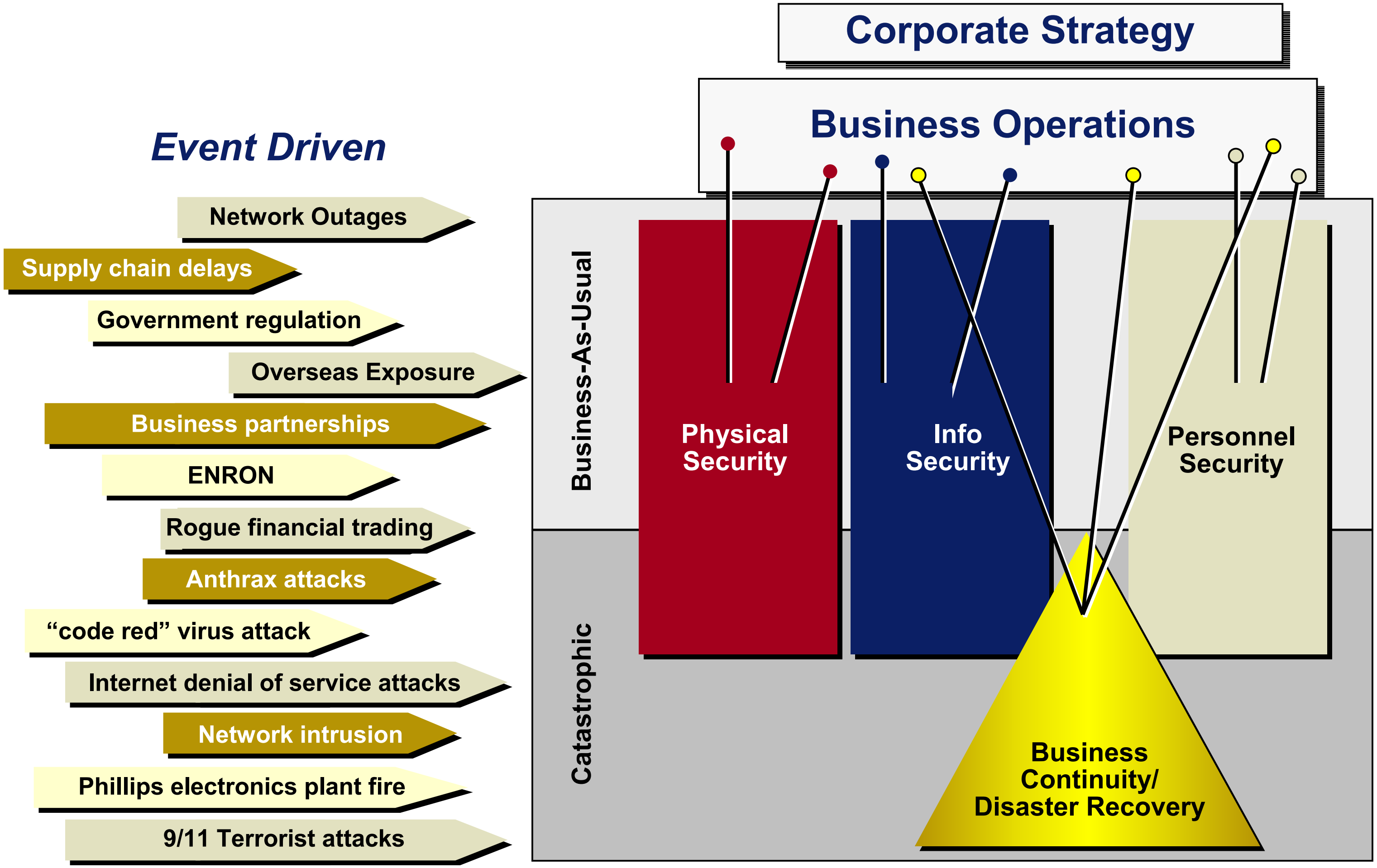
- Like most staff who work in this field, she is all about planning
- A lot of this discipline is about relocation and backup sites
- Recently, in the post 9/11 world, more than any other area of security, firms are beginning to worry
- But this field until recently was arcane and isolated

Some observations:

- These folks don’t know one another very well and don’t work together
- In many firms and agencies, the traditional focus of security has been in the physical area
- Other areas of security operate in silos, with dysfunctionalities often emerging
- The languages and cultures of each of the disciplines are different, making clear coordination and comprehensive security approaches and solutions rare
- No amount of technology will overcome these discontinuities without leadership, perspective and management coordination

Traditional Risk Framework

… where risk mitigation is event-driven, imposes point solutions on business operations, and relies on corporate policies for consistency and alignment

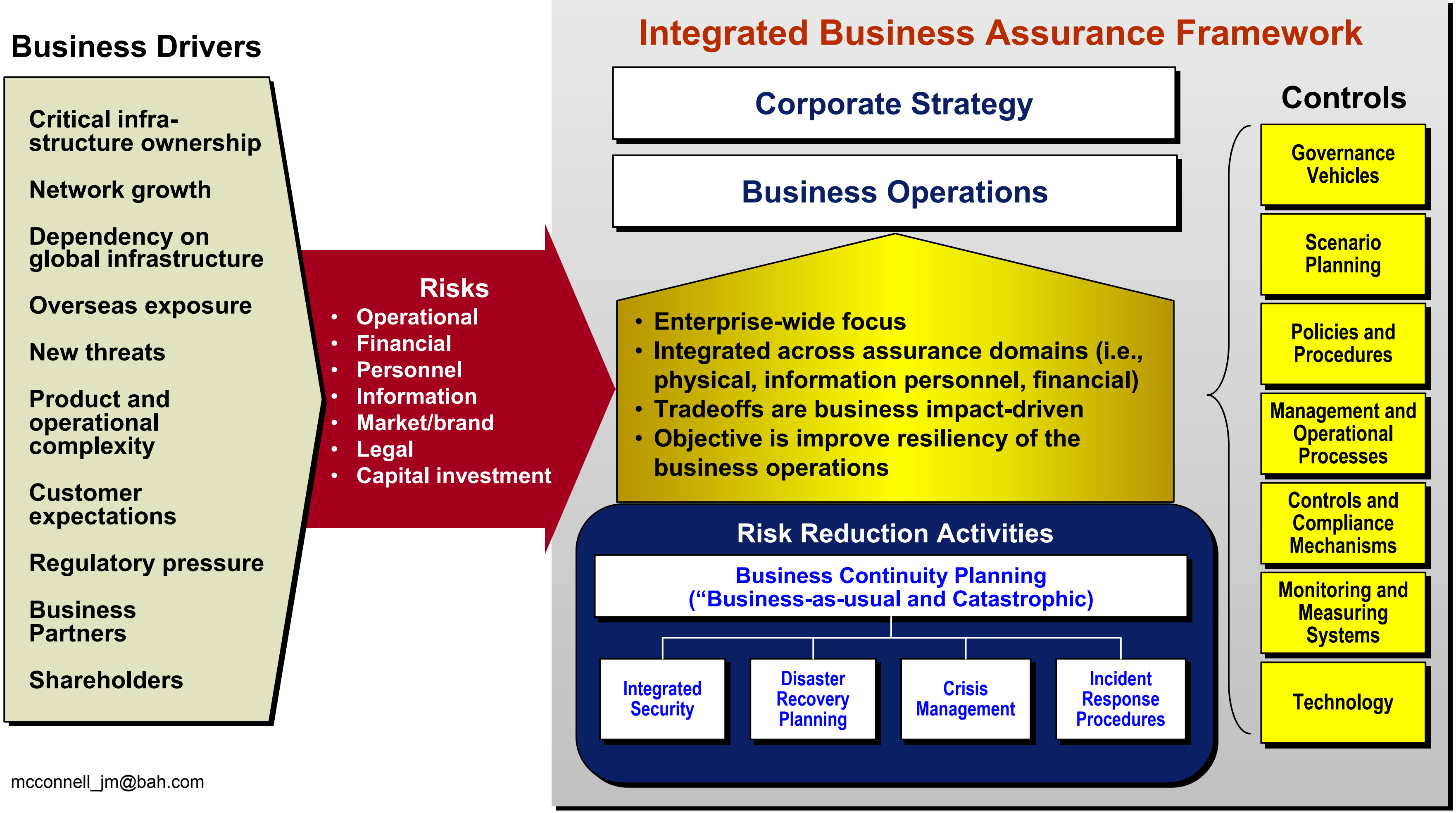


A better interim state:

“The way we’re moving”

Integrated Business Assurance Framework

… where risk reduction activities are dynamically linked to business operations to implement corporate strategy



Business Drivers

- Critical infra-structure ownership
- Network growth
- Dependency on global infrastructure
- Overseas exposure
- New threats
- Product and operational complexity
- Customer expectations
- Regulatory pressure
- Business Partners
- Shareholders

Risks

- Operational
- Financial
- Personnel
- Information
- Market/brand
- Legal
- Capital investment

Integrated Business Assurance Framework

Corporate Strategy

Business Operations

- Enterprise-wide focus
- Integrated across assurance domains (i.e., physical, information personnel, financial)
- Tradeoffs are business impact-driven
- Objective is improve resiliency of the business operations

Risk Reduction Activities

Business Continuity Planning
("Business-as-usual and Catastrophic)

- Integrated Security
- Disaster Recovery Planning
- Crisis Management
- Incident Response Procedures

Controls

- Governance Vehicles
- Scenario Planning
- Policies and Procedures
- Management and Operational Processes
- Controls and Compliance Mechanisms
- Monitoring and Measuring Systems
- Technology

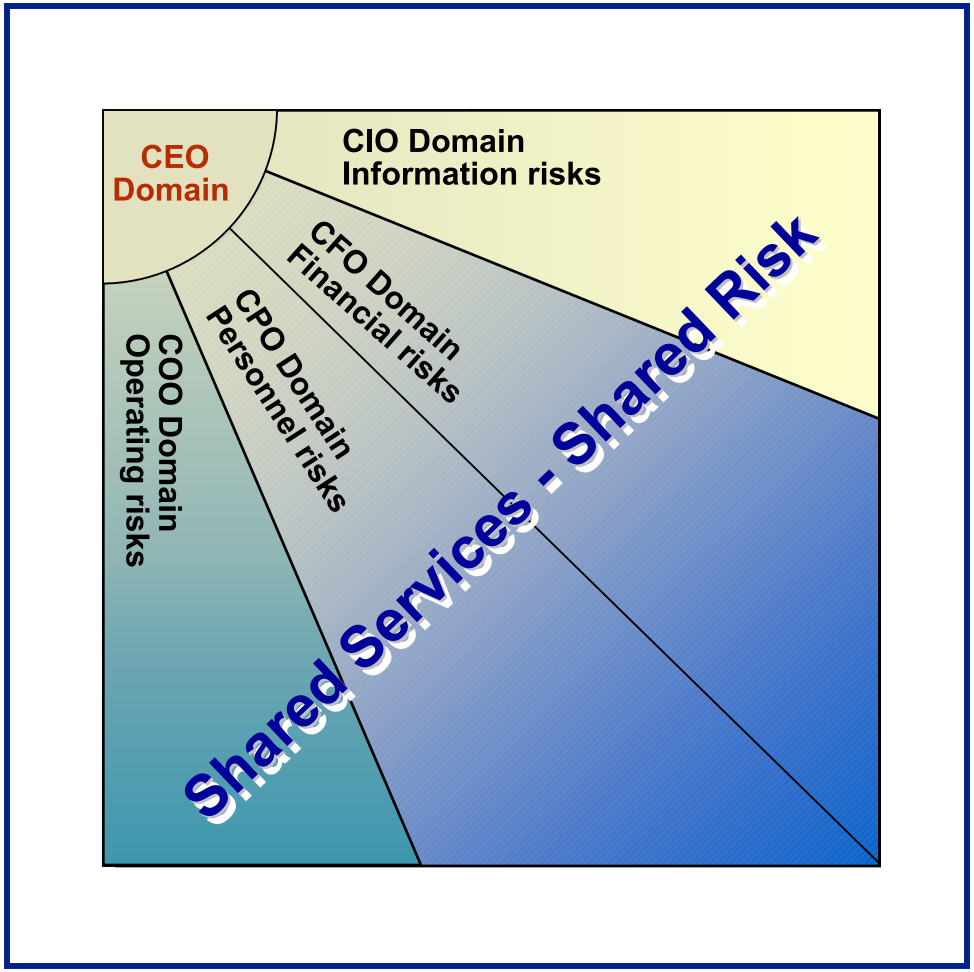
mcconnell_jm@bah.com

A future state:

“The way we should ultimately be”

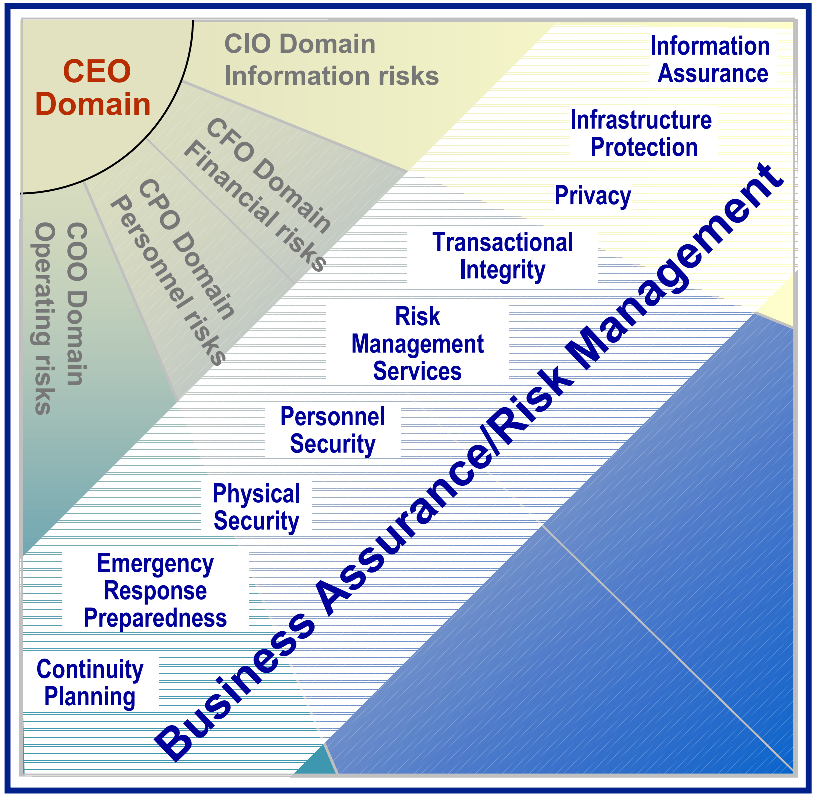
Given today's threats, agency heads and CEOs need an even more comprehensive risk management framework

- Risk is stove-piped by nature within the traditional organizational domains
- The domains, however, typically share infrastructure services and have complex interdependencies and linkages
- Business resilience, in today's new threat environment, requires cross cutting solutions that manage risks and assures operational effectiveness
- There is need for internal and external risk management planning

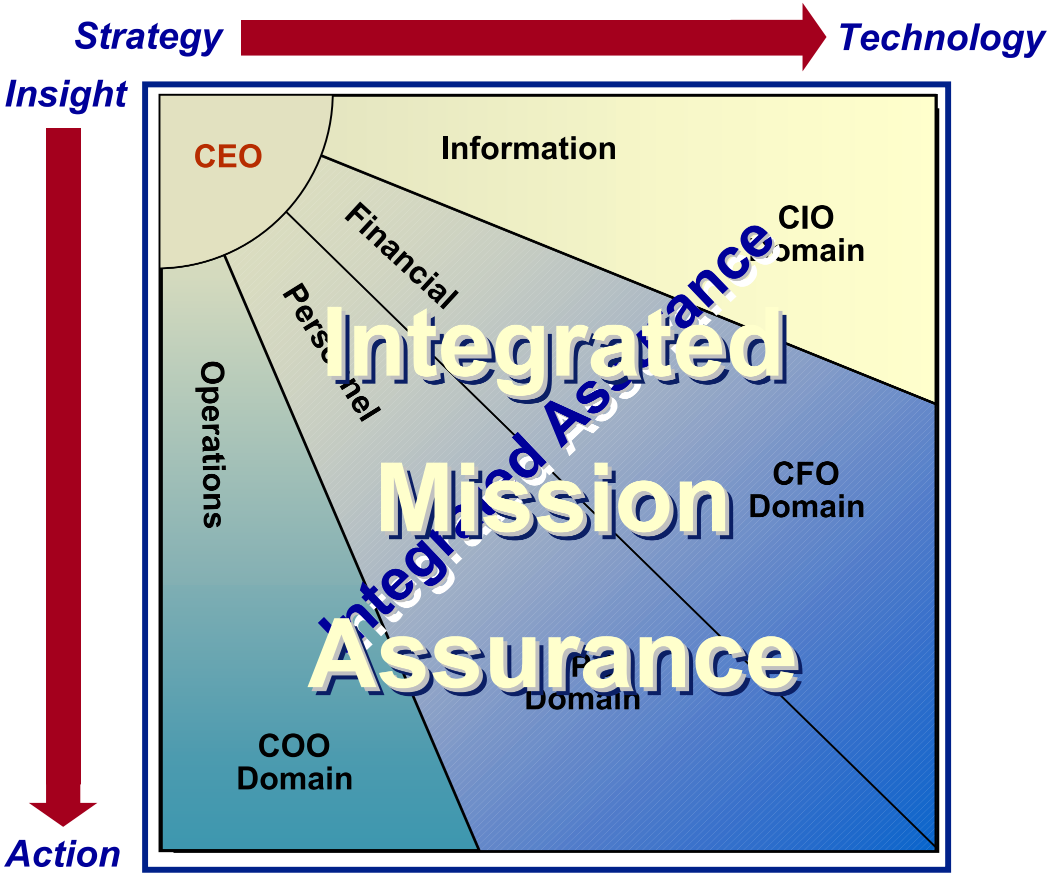

CEO Domain
CIO Domain Information risks
CFO Domain Financial risks
CPO Domain Personnel risks
COO Domain Operating risks
Shared Services - Shared Risk

A Business Assurance/Risk Management program should reconcile, synchronize and integrate an organization's operational effectiveness and long term viability

- The new enterprise dynamic wo feature:
  - Trust
  - Collaboration
  - Shared information
  - A common view
  - Effective security
  - Business resilience
- Enhances overall business continuity management and emergency response preparedness
- Steps:
  - Realistic Vulnerability Assessment
  - Risk Mitigation Plan and Implementation
  - Business Adaptation for growth/brand protection


CEO Domain
CIO Domain Information risks
CFO Domain Financial risks
CPO Domain Personnel risks
COO Domain Operating risks
Information Assurance
Infrastructure Protection
Privacy
Transactional Integrity
Risk Management Services
Personnel Security
Physical Security
Emergency Response Preparedness
Continuity Planning
Business Assurance/Risk Management

The leadership suite's *Assurance Domains* need to share information and collaborate in unprecedented ways to adapt to the new operating realities



Preparing for a new operating reality could start with one or more program elements of Integrated Business Assurance

- **Mission Analysis and Integration:** baseline assessment and negotiated understanding of economic and operational performance measures
- **Integrated Security:** blend of cyber, physical, personal activities
- **Consolidated Risk Management:** across all assurance domains (COO, CFO, CPO, CIO)
- **Business Continuity Planning:** business impact assessment
- **Decision Support System:** situational awareness using automated tools and command center engineering practices
- **Performance Optimization:** actively managing against measures for the enterprise mission, facilitates eBusiness migration, mergers and acquisitions, new technology
- **Indications and Warnings:** forecast of political, economic and business impacts
- **Crisis Communications:** enables management of key operational, Issues Management
- **Transformational Leadership:** turning crisis into opportunity

Summary

- The World Is More Complicated and So Therefore Is Risk Management

- We Often Look To Technology To Solve Our Most Pressing Security Problems, But It Is Most Often Leadership, Perspective and Management Coordination Which Are Far More Important

- The Big Winners Will Be Firms and Agencies Which Take the Broadest View of Risk Management, Integrating Not Only Traditional Security Disciplines But Also Other Areas of Risk and Connecting Them To the Business and Its Mission